La Guardia di Finanza non c'entra!

Enrico Tonello,
Ricercatore Anti Malware

Sicurezza sempre in pericolo: il virus FakeGfF rapisce il computer per estorcere 100 Euro. In guardia!

IL NUOVO virus FakeGdF si sta diffondendo a macchia d'olio, e spesso lascia a bocca aperta gli utenti più vulnerabili sul piano tecnologico o su quello psicologico, ottenendo livelli di successo record! Si tratta di un virus/malware inquadrabile nella tipologia dei *ransomware* (ricattatori).

I *RANSOMWARE* sono una tipologia di Malware che bloccano l'accesso al computer infetto chiedendo un riscatto per rimuovere l'infezione o per il suo sblocco.

FAKEGDF, IL cui capostipite è il Trojan.Win32.FakeGdf.A, ora giunto alla variante .DC, blocca il computer collegandosi ad un sito in Russia (hxxp://83.69.236.38), visualizzando sul PC colpito una falsa segnalazione della Guardia di Finanza. L'obiettivo è indurre la sua malcapitata vittima, che si trova con il computer "bloccato", al pagamento, tramite Voucher Ukash, di una sanzione comminatagli dalla Guardia di Finanza italiana.

LA VIDEATA che compare subito dopo che il PC si collega al sito russo viene visualizzata a tutto schermo e non permette più alcuna interazione con il computer. L'utente ha solo la possibilità di inserire i codici pin di Ukash o di Paysafe, oppure di Cliccare sull'indirizzo email "deposito@cyber-gdf.net".

» continua a, **PG. 26**

Speciale BPM & Process Integration

Il BPM per ridurre i costi e migliorare la qualità dei processi aziendali

A cura di Aurelio Carlone

Sintesi ragionata dei risultati di una ricerca condotta recentemente dalla società di analisi Gartner su circa 600 aziende di varie parti del mondo.

COME SONO stati condotti e in quali aree sono stati impiegate le soluzioni BPM sviluppate in circa 600 società, distribuite nelle più importanti aree geo-economiche del mondo? Quali i principali risultati raggiunti e le misurazioni adottate?

PARTENDO DA tali quesiti, Gartner ha condotto un'articolata indagine, i cui risultati sono stati sintetizzati in uno studio dedicato ad essa, quindi ripresi ed illustrati nel corso del BPM Summit tenutosi lo scorso Marzo a Londra.

Per quali Processi/Aree Adottare il BPM?

SECONDO L'INCHIESTA Gartner, i processi "*Customer Facing*" sono stati indicati cone l'area principale (50%) per la quale si è adottato o si sta adottando il BPM. L'approdo al BPM è giustificato anche dalla necessità di gestire meglio i progetti mirati sul "Task Management" (49%). In altre parole, si vuole ridurre il tempo che i dipendenti dedicano alla compilazione di classici "rapportini" sulle attività svolte ("Time-Sheet"), delle "Note-spese", delle "Performance-Review", per dedicarne di più ad altre attività maggiormente utili.

LA NECESSITÀ di guardare con più attenzione allo svolgimento delle attività interne all'azienda, puntando ad incrementare l'efficienza operativa dell'azienda, si riscontra in modo più consistente tra le società che hanno appena cominciato a muovere i primi passi nel BPM.

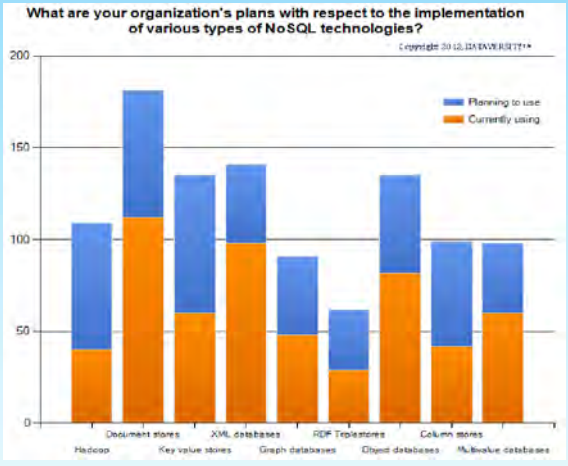
» continua a, **PG. 14**

NoSQL: i Dati di Dataversity Indicano Che è una Realtà!

Proponiamo in anteprima esclusiva i risultati della ricerca promossa su scala mondiale tra Febbraio e Marzo 2012 dall'azienda di formazione OnLine californiana.

NEI GIORNI scorsi, abbiamo ricevuto in anteprima i dati frutto di un'indagine condotta a livello mondiale tra febbraio e marzo 2012, su un campione di circa 500 imprese di varie dimensioni, utenti o prossimi utenti di strumenti di interrogazione e analisi dei dati che non fanno uso delle tradizionali tecnologie SQL.

DI TECNOLOGIE NoSQL - che a secondo dei punti di vista sta sia per No all'SQL, sia per Non solo SQL - abbiamo già parlato più volte su Toolnews, spesso in associazione alla gestione dei "Big-Data", ma non solo. Si tratta di strumenti che vanno



» continua a, **PG. 28**

« La Guardia di Finanz non c'entra! - da pag. 3

IL SITO russo riporta il logo della Guardia di Finanza, avvertendo l'utente che dal suo computer sono state eseguite operazione illecite quali il Download di pornografia minorile o l'invio di Spam di tipo "terroristico".

la procedura sopra citata sarebbe del tutto illegale, inserendo un qualsiasi codice non si viene portati a nessuna pagina e in alcun modo si riceverebbero le istruzioni o i codici per sbloccare il proprio computer. La

E' CHIARO che a queste organizzazioni interessa diffondere le loro creazioni il più possibile così da infettare il maggior numero di utenti aumentando, in questo modo, la possibilità che qualcuno cada nella

modificato ad arte anche più volte nell'arco della stessa giornata di modo da renderlo invisibile ai più comuni Antivirus sia pure aggiornati alla versione più recente.

COME SE ciò non bastasse, i suoi creatori, hanno ben pensato anche di rendere disponibili nuovi Payload (interfacce), che invitano l'ignaro utente al pagamento di sanzioni relative a:

> Pirateria informatica;
> BUNDES POLIZEI;
> Carabinieri
> Polizia Postale e delle Comunicazioni.

QUESTI "BUONTEMPONI" stanno quindi sviluppando una vera e propria industria della truffa OnLine che sfrutta ad arte le azioni del governo per il contenimento dell'evasione fiscale nel nostro Paese, spacciandosi in modo fraudolento proprio per queste organizzazioni statali (Guardia di Finanza, Polizia Postale, Carabinieri etc. etc.).

A QUESTO punto il computer risulta bloccato e per ripristinarlo alle funzionalità originarie, viene chiesto di pagare una multa di 100 Euro tramite Ukash oppure Paysafecard, con le relative istruzioni di pagamento.

NEL CASO il sistema di pagamento vada in errore, il Malware raccomanda di inviare una e-Mail con i codici di Ukash o di Paysafecard a deposito@cyber-gdf.net.

NATURALMENTE, LA multa è solo un pretesto per rubare dei soldi all'utente capitato in questa situazione, tutte le affermazioni e informazioni presenti sul sito a cui si viene portati sono false e a scopo di truffa. In questi casi non si deve assolutamente pagare alcuna cifra di denaro. Oltre al fatto che chiaramente la Guardia di Finanza non "riscuote" multe bloccando i computer degli utenti e

somma pagata verrebbe solamente riscossa dal truffatore e il computer sarebbe comunque nella stessa situazione di prima.

QUESTO RANSOMWARE sfrutta l'approccio emozionale che fonda le sue radici nell'ingegneria sociale, con l'obiettivo di indurre attraverso la videata, scritta in un italiano in qualche punto un po' stentato, le sue vittime ad effettuare dei pagamenti a favore dell'organizzazione criminal-informatica che ha architettato questa truffa.

L'OBIETTIVO È carpire i codici dei voucher UKASH che l'utente si è procurato acquistandoli attraverso i punti vendita. In Italia, i voucher UKASH sono acquistabili attraverso le ricevitorie SISAL, quindi la possibilità che più di qualche malcapitato sia indotto al pagamento non è poi così remota.

trappola e sia indotto ad effettuare il pagamento.

IL COSIDETTO Payload di questo *ransomware*, cioè gli effetti visibili dello stesso, sono riportati nell'immagine 1). Purtroppo, sebbene il Payload sia il medesimo, cioè l'interfaccia possa rimanere la stessa, il File portatore/generatore dell'infezione, cioè quello che dovrebbe essere intercettato preventivamente dall'Antivirus viene

LE NUOVE varianti del FakeGdF inibiscono il riavvio del PC anche in modalità provvisoria, rendendo ancor

più difficoltosa la sua rimozione.

IL FAKEGDF negli ultimi mesi ha utilizzato numerosi File portatori modificati ad arte, anche più volte al giorno, per non essere identificati/bloccati dai più comuni Antivirus in uso; tra questi ne riportiamo un elenco che, per ovvi motivi, non è da considerarsi esaustivo e, con tutta probabilità, è in continua evoluzione:

- 0.[numero casuale].exe
- WPBT0.DLL
- seti0.exe
- ms[nome casuale].exe oppure .com, .pif, .scr;
- msuu0.exe;
- hj8ol0.exe;
- taskinit.exe;
- ms.exe;
- ch8l0.exe;
- cgs8h0.exe.

Ma...il Virus, da Dove Arriva?

PER QUANTO riguarda questo *Ransomware* il C.R.A.M. Centro Ricerche Anti Malware di TG Soft ha verificato che alcuni dei veicoli di diffusione sono:

1. e-Mail contenenti "interessanti" e/o "invitanti" link;
2. Collegamento a pagine web di siti compromessi. In altre parole la pagina di accesso al sito è stata violata e modificata ad arte di modo che il suo caricamento proceda ad eseguire il file diffusore del virus/malware che, come già evidenziato viene variato/modificato ad arte anche più volte al giorno per non essere identificato dai più comuni antivirus in uso;
3. Banner pubblicitari il cui codice originale è stato modificato ad arte per diventare anche esecutore del file portatore dell'infezione. Questa modalità di diffusione è stata verificata su alcune nuove varianti del virus della Guardia di Finanza e anche dei suoi successivi "fratellini" della Polizia e dei Carabinieri...
4. Viene installato da altri Malware, come il TDL4 (Trojan Downloader) che ha precedentemente infettato il PC.

L'UTENTE EDUCATO all'uso di un Antivirus aggiornato e che pensa che questo possa bastare per difendersi da questa tipologia di Ransomware si trova incredulo nel vedere il suo computer colpito, magari a ripetizione, da queste tipologie di virus/malware e si chiede come mai questo continui a succedere seppur il suo Antivirus sia costantemente aggiornato.

IL PROBLEMA, come detto, sta nel fatto che non si tratta sempre e comunque dello stesso virus/malware ma si tratta di un Ransomware che, sebbene possa palesarsi con la stessa veste/interfaccia, viene inoculato nel PC da File modificati ad arte proprio per non essere identificati e quindi bloccati preventivamente dai più comuni Antivirus in uso.

E ALLORA, come fare ad avere delle segnalazioni dell'insinuarsi nel nostro PC e/o nella nostra rete locale di qualche nuova variante del Ransomware della GdF e dei suoi fratellini ma soprattutto di eventuali loro varianti? Per avere segnalazioni dell'intrusione di eventuali nuove varianti, il C.R.A.M. di TG Soft mette a disposizione, sia in ambito privato sia aziendale, Vir.IT eXplorer Lite –Free Edition- come integrazione di tutti gli AntiVirus normalmente presenti negli ambienti Windows.

VIR.IT EXPLORER Lite –Free Edition-, liberamente prelevabile dal sito www.tgsoft.it, ha le seguenti caratteristiche:

> E' liberamente utilizzabile sia in ambito privato/domestico sia in ambito aziendale/professionale su tutte le piattaforme Microsoft Windows, da Win95 a Win7, incluse tutte le versioni Server;
> E' interoperabile con gli eventuali altri Antivirus già presenti sul PC, senza doverli disinstallare.
> Dispone di aggiornamento automatico sia del motore che delle firme, senza limitazioni temporali.

VIR.IT LITE Monitor modulo che sovrintende all'aggiornamento del software sia come motore sia come firme di identificazione e che gestisce le scansione schedulate/pianificate integra la tecnologia INTRUSION DETECTION in grado di segnalare le intrusioni di eventuali virus/malware di nuova generazione che si pongono in esecuzione e, anche se il computer dovesse essere bloccato da una nuova variante del FakeGdF, con una combinazione di tasti [CTRL]+[ALT]+[SHIFT]+[Z], sarà in grado di portarsi in primo piano scavalcando il virus per poter inviare il file sospetto individuato dall'Intrusion Detection al C.R.A.M. di TG Soft per l'analisi e l'eventuale aggiornamento del software per l'univoca identificazione e rimozione dell'agente Malware di nuova generazione. Il tutto viene reso disponibile nei successivi aggiornamenti rilasciati gratuitamente agli utenti.

VIR.IT EXPLORER Lite –Free Edition- quindi è un Antivirus gratuito che è consigliabile installare, e mantenere in uso, ad integrazione della protezione offerta al vostro Antivirus, sia che si tratti di un Antivirus gratuito, o presunto tale, ma anche e soprattutto se si utilizza un Antivirus regolarmente licenziato e quindi acquistato.

Consigli Pratici per Risultare Meno Vulnerabili

> PER TUTTI GLI UTENTi: Oltre all'utilizzo sistematico di Vir.IT eXplorer Lite ad integrazione di eventuali Antivirus già uso sui computer, il C.R.A.M. ha verificato che la diffusione delle nuove varianti può avvenire attraverso Banner pubblicitari che una volta visualizzati sul PC collegandosi anche a siti istituzionali o considerati affidabili, procedono automaticamente ad attivare file portatori di nuove varianti del Ransomware. Per questo è consigliabile utilizzare un Browser che permetta di escludere dalla visualizzazione della pagina i Banner pubblicitari tra questi segnaliamo Mozilla FireFox o eventualmente Google Chrome con l'utilizzo di componenti aggiuntivi come AD-BLOCK PLUS.

> PER UTENTI ESPERTI: una buona pratica è bloccare durante la navigazione la visualizzazione di pagine che prevedono l'esecuzione di codice Javascript. Possibilità che è disponibile sulla maggior parte dei Browser più comuni (IE, Mozilla Firefox etc. etc.). Naturalmente sarà discrezione dell'utente procedere a sbloccare l'esecuzione del codice Javascript limitatamente alla pagina o al sito a cui si stà collegando poiché questo, in quanto sito noto e/o istituzionale, non dovrebbe dare adito all'esecuzione/scaricamento di file malevoli. Naturalmente se anche siti noti o istituzionali fossero stati, a loro insaputa, compromessi l'esecuzione del Javascript potrà dare seguito all'esecuzione/scaricamento di eventuali file malevoli.

CONCLUDENDO PER cercare di difendersi da questa tipologia di minacce, un Antivirus non basta più, ed è necessaria, sempre e comunque, da parte dell'utente, la consapevolezza che dietro qualsiasi Link o pagina Web può sempre e comunque celarsi in ogni momento qualche minaccia di nuova generazione che l'Antivirus in uso può non essere in grado di identificare e quindi tantomeno di rimuovere. www.tgsoft.it/italy/cram.asp.